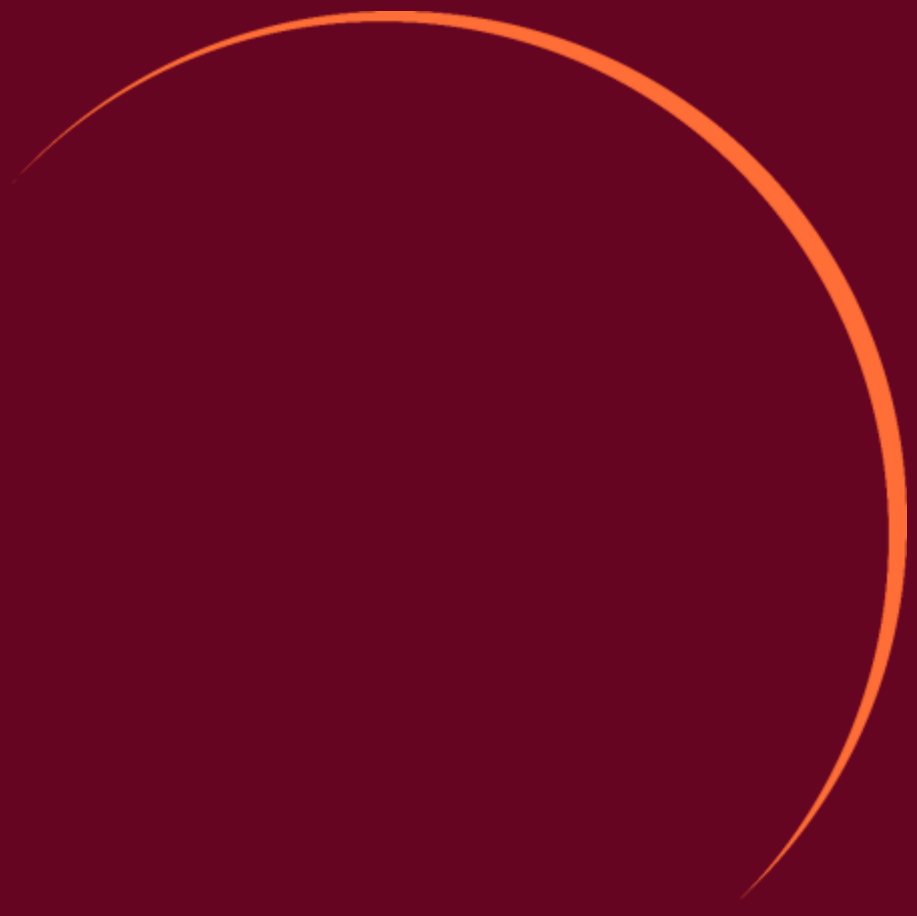
МОНИТОРИНГ ТРАФИКА И ЗАЩИТЫ ОТ DDOS-АТАК

КРУГЛОСУТОЧНАЯ ЗАЩИТА КАНАЛОВ СВЯЗИ И ОНЛАЙН-РЕСУРСОВ ОТ DDOS-АТАК ДЛЯ ОРГАНИЗАЦИЙ ПО ПОДПИСКЕ



МОСКВА, 2024

RT-SOLAR.RU

СОДЕРЖАНИЕ

СПИСОК ИЛЛЮСТРАЦИЙ

СПИСОК ТАБЛИЦ

1. DDOS-АТАКА КАК ИНСТРУМЕНТ КИБЕРПРЕСТУПНИКОВ

1.1. ЧТО ТАКОЕ DDOS-АТАКА

Сегодня интернет – неотъемлемая часть функционирования практически любой организации. С учетом этого обстоятельства доступность онлайн-ресурсов становится для них важным условием поддержания рабочих процессов, поскольку любые сбои могут повлечь за собой различные риски и даже финансовые потери.

Киберпреступность не стоит на месте: изобретаются новые инструменты и совершенствуются методы атак. Один из наиболее распространенных инструментов киберпреступников – это DDoS-атаки, популярность которых связана с простотой организации и низкой стоимостью их реализации. Минимальная стоимость такой атаки составляет 50 долларов, а заказать ее не составляет труда – в интернете активно появляются предложения по организации DDoS-атаки как услуги.

DDoS-атака – это целый набор действий злоумышленников, направленных на нарушение работоспособности инфраструктуры компании и клиентских сервисов. Хакеры с помощью специальных инструментов создают множественные запросы к интернет-ресурсу, значительно увеличивая нагрузку на него, и таким образом вызывают отказ в обработке легитимных запросов. Тип атаки зависит от элемента инфраструктуры, на который она направлена, и технологии самой атаки:

- Объемные DDoS-атаки пытаются использовать полосу пропускания либо внутри целевой сети, либо между целевой сетью/службой и остальной частью интернета. Такие атаки приводят к сбою в работе сетевых устройств и серверов.
- Атаки типа TCP State-Exhaustion Attacks на сетевые устройства эксплуатируют функциональность контроля состояния сессий TCP и нацелены на заполнение таблицы состояний TCP фиктивными соединениями. Данный тип атак обычно выводит из строя файрволы и веб-серверы.
- Атаки уровня приложений нарушают работу корпоративных приложений или клиентских онлайн-сервисов. Как следует из названия, этот тип атак нацелен на приложения и протоколы передачи данных, например HTTP(S), работающие на прикладном уровне.

DDoS-атаки выводят из строя онлайн-ресурсы компании, тем самым останавливая ее работу, и способны нанести непоправимый вред репутации, не говоря уже о финансовых потерях или упущенной прибыли. Подобные атаки происходят в самый неподходящий момент, и, если меры по защите от них не приняты заблаговременно, они парализуют бизнес-процессы компании.

Нарушение доступности онлайн-ресурсов часто является отправной точкой для развития комбинированной атаки, нацеленной на кражу конфиденциальной информации и персональных данных, заражение хостов или выведение из строя оборудования.

По данным ГК «Солар», за I полугодие 2024 года:

в 4 раза

выросла частота ежедневных DDoS-атак

1,2 Тбит/с

мощность самой крупной зафиксированной атаки

35 дней

длилась самая долгая атака в отчетном периоде

Чтобы организовать надежную защиту от DDoS-атак собственными силами, недостаточно дорогостоящего оборудования и квалифицированных специалистов. Проблема заключается в том, что нужно принять и обработать весь поток трафика, а также качественно профилировать атаки. Для своевременного выявления атаки и нейтрализации возможных последствий организациям требуется современное и надежное средство.

1.2. КТО ПОДВЕРЖЕН DDOS-АТАКАМ

В первую очередь уязвимы перед DDoS-атаками компании, чьи бизнес-процессы напрямую связаны с онлайн-коммуникациями.

Среди отраслей и организаций, наиболее подверженных DDoS-атакам, можно выделить следующие:

- Финансы
- Промышленность
- Ретейл
- Стриминговое вещание
- ТЭК
- Транспорт
- Субъекты КИИ

1.3. КАК DDOS-АТАКА МОЖЕТ НАВРЕДИТЬ ОРГАНИЗАЦИИ

Самая распространенная проблема в случае DDoS-атаки на компанию – это остановка бизнес-процессов, связанных с использованием интернета. В зависимости от типа атаки ее мишенью становятся либо серверы, либо пропускная способность сети. Как результат, онлайн-ресурсы компании становятся недоступными для легитимных пользователей до предотвращения DDoS-атаки либо до ее окончания, что приводит к невозможности выполнить заказ, срыву сроков поставки и т. п.

Значительный урон компании могут нанести репутационные риски. К этой же категории относится отток и потеря клиентов. Особенно актуален такой тип риска для компаний, онлайн-ресурсы которых должны быть доступны круглосуточно.

Наибольший вред компаниям наносят прямые финансовые потери, а также правовая ответственность, которая может наступить в случае несоответствия нормативно-правовым актам в сфере кибербезопасности либо в случае невыполнения договорных обязательств и последующих исков.

Ущерб от DDoS-атак является следствием реализованных рисков. Например, по информации «РИА Новости», в 2010 году был выведен из строя сайт платежной системы Assist посредством DDoS-атаки, в результате чего у «Аэрофлота», заключившего контракт с Assist, возникли сложности с продажей авиабилетов через интернет и авиакомпания потеряла 146 миллионов рублей.

Существуют различные типы рисков:

РЕПУТАЦИОННЫЕ РИСКИ

- Падение биржевых индексов компании
- Снижение стоимости бренда
- Недоступность публичной корпоративной информации
- Негатив в СМИ
- Отток клиентов, их переход к конкурентам

ТЕХНОЛОГИЧЕСКИЕ РИСКИ

- Простой производства
- Недоступность корпоративных ресурсов для сотрудников компании

ФИНАНСОВЫЕ РИСКИ

- Расторжение контрактов
- Упущенная прибыль
- Отмена аукционов
- Срыв сделок
- Потеря денежных средств биржами и инвестиционными компаниями, а также их клиентами

ПРАВОВЫЕ РИСКИ

- Ответственность за невыполнение требований регуляторов
- Ответственность за нарушение контрактных обязательств

2. ПЕРЕЧЕНЬ НОРМАТИВНЫХ ТРЕБОВАНИЙ

Сервис защиты от DDoS-атак помогает клиентам выполнять требования следующих нормативно-правовых актов РФ:

- Приказ ФСТЭК России № 489 и ФСБ России № 416 от 31 августа 2010 г. «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования» в части выполнения п. 11 по поддержанию целостности и доступности информации.
- Приказ ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» в части выполнения указаний по защите информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы (ЗИС 22).
- Приказ ФСТЭК России № 239 от 25 декабря 2017 г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» в части предотвращения вторжений (компьютерных атак) и обеспечения доступности значимых объектов и требования к защите от угроз, направленных на отказ в обслуживании (DOS-, DDoS-атаки) (ЗИС 34).
- Приказ ФСБ России № 196 от 6 мая 2019 г. «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» в части выявления компьютерных инцидентов и реагирования на них, работы с артефактами атаки и отсутствием недекларированных возможностей в используемом программном обеспечении.
- Приказ ФСТЭК России № 31 от 14 марта 2014 г. «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» в части выполнения указания по защите от угроз, направленных на отказ в обслуживании (DOS-, DDoS-атаки) (ЗИС 34).
- ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» в части реализации мер защиты «Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным осуществлением атак типа "отказ в обслуживании", предпринимаемых в отношении ресурсов доступа, размещенных в вычислительных сетях финансовой организации, подключенных к сети Интернет» (ВСА.8) и «Блокирование атак типа "отказ в обслуживании" в масштабе времени, близком к реальному» (ВСА 9).
- ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» в части реализации мер защиты в соответствии с разделами А.12.1.3, А.12.4.1, А.14.1, А.14.2, А.12.6, А.13.1, А.15.1.3, А.16, А.17.

Сервис также учитывает требования методического документа «Методика оценки угроз безопасности информации», утвержденного ФСТЭК России 5 февраля 2021г., в части п. 4.5 «Для определенных информационных ресурсов и компонентов систем и сетей должны быть определены виды воздействия на них, которые могут привести к негативным последствиям», согласно которым в отношении вида воздействия «отказ в обслуживании компонентов (нарушение доступности)» необходимо реализовать программно-технические меры защиты информации в ИС по защите от атак типа «распределенный отказ в обслуживании» (DDoS).

3. ОПИСАНИЕ СЕРВИСА

3.1. НАЗНАЧЕНИЕ

ГК «Солар» предлагает современное решение – сервис круглосуточной защиты каналов связи и онлайн-ресурсов от DDoS-атак для организаций любых регионов по подписке.

Сервис мониторинга трафика и защиты от DDoS-атак позволяет фильтровать на магистральном уровне атаки суммарной мощностью до 5 Тбит/с и обеспечивает таким образом круглосуточную доступность интернет-ресурсов пользователям.

Основное преимущество сервиса – эшелонированная защита от DDoS-атак, которая позволяет защитить как каналы, так и сетевую инфраструктуру компании. Сервис фильтрует атаки уровня L3/L4 по модели OSI. Этим занимается специальный центр очистки. При этом фильтрация атаки никак не влияет на доступность инфраструктуры, приложений и онлайн-сервисов для легитимных пользователей. Архитектура решения исключает потерю трафика при переключении на центр очистки и имеет полное георезервирование.

Сервис можно подключить как для одной организации, так и для компании с множеством офисов или дочерними предприятиями, распределенными географически. Сервис доступен в рамках канала передачи данных и основной автономной системы ПАО «Ростелеком».

Обработка трафика производится на территории России.

3.2. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

В ходе предоставления Услуги осуществляется:

- Мониторинг и анализ телеметрии на предмет наличия аномалий в трафике:
  1) выявление и регистрация атак;
  2) первичная обработка выявленной атаки: регистрация инцидента, базовая диагностика (обработка ложных срабатываний сценария), уточнение критичности, информирование клиента о факте обнаружения инцидента (по согласованию).
- Перенаправление трафика в центр очистки посредством изменения маршрута следования трафика как в автоматическом, так и в ручном режиме.
- Реагирование и противодействие атаке:
  1) организация и координация работ по фильтрации трафика и блокированию атак на уровне исполнителя;
  2) оперативное изменение политик фильтрации для блокирования атаки или снижения ее воздействия;
  3) блокирование атаки методами BGP FlowSpec и Blackhole на магистральном оборудовании сети «Ростелеком» в случае невозможности ее предотвращения средствами ПАК-фильтрации.

Сервис позволяет:

- Формировать необходимые аналитические отчеты и выгружать данные, касающиеся:
  1) конкретных атак;
  2) векторов атаки;
  3) методов очистки (подавления атаки);
  4) зафиксированных атак за выбранный период времени.

3.3. РЕШАЕМЫЕ ЗАДАЧИ

Сервис мониторинга трафика и защиты от DDoS-атак обеспечивает:

- Круглосуточный мониторинг и отражение атаки в автоматическом режиме

Сервис анализирует трафик 24/7, и в случае подозрения на атаку трафик направляется в центр очистки. Это позволяет избежать недоступности ресурсов и остановки бизнеса.

- Отражение массированных атак

  Сервис фильтрует атаки уровня L3/L4 объемом до 5 Тбит/с, что позволяет отражать объемные атаки, многократно превышающие самые сильные из зафиксированных в России.

- Доступность онлайн-сервисов во время обработки трафика

  Фильтрация атаки не влияет на доступность инфраструктуры, приложений и сервисов для пользователей. Архитектура сервиса обеспечивает его отказоустойчивую реализацию.

- Защиту от DDoS-атак для всех офисов

  Собственная защищенная сеть, охватывающая всю страну, обеспечивает простую масштабируемость при подключении новых офисов.

3.4. ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ СЕРВИСА

Сервис защиты от DDoS-атак реализован на распределенной платформе фильтрации, развернутой в сети «Ростелеком», и включает в себя специализированные модули:

- Модуль анализа трафика (анализатор)

  Используется для круглосуточного мониторинга состояния сети и, в частности, различных параметров трафика, адресованного клиенту. Модуль позволяет создавать профиль трафика, основанный на получаемой от клиента информации. Профиль трафика используется для обнаружения аномалий, является динамическим и постоянно обновляется в реальном времени. Это позволяет анализатору в автоматическом режиме сигнализировать о возникновении аномалии защищаемого ресурса.
  Трафик не пропускается непосредственно через модуль анализа, маршрутизация не изменяется.
  При подключении для анализа трафика по умолчанию используется один из преднастроенных профилей, выработанный в рамках оказания сервиса клиентам с подобными параметрами трафика.
  Если клиент предоставляет точные параметры защищаемой интернет-инфраструктуры, может быть настроен индивидуальный профиль трафика. Для этого у клиента запрашивается следующая информация:

ТАБЛИЦА 1. ПРИМЕР ПАРАМЕТРОВ ИНТЕРНЕТ-ИНФРАСТРУКТУРЫ, ЗАПРАШИВАЕМЫХ У КЛИЕНТА ДЛЯ НАСТРОЙКИ ИНДИВИДУАЛЬНОГО ПРОФИЛЯ ТРАФИКА

№	Наименование ресурса	Доменное имя ресурса, FQDN (если есть)	IP-адрес(а) ресурса	Протокол	Разрешенные порты	
					dst	src
1	Веб-сервер	example.ru	10.10.10.10	TCP	80, 443	1024..65535
2			10.10.10.10	ICMP		
3	DNS		10.10.20.10/29, 172.16.1.10	UDP,TCP	53	1024..65535
N						

- Модуль фильтрации трафика (очиститель)

  Фильтрует нежелательный трафик в случае выявления атаки. Весь трафик, адресованный защищаемому ресурсу, перенаправляется на специальное оборудование. Оно производит глубокий анализ пакетов и фильтрацию вредоносного трафика (например, могут быть отфильтрованы нелегитимные фрагменты пакетов, сгенерированные злоумышленником). В результате этого паразитный трафик отбрасывается, а легитимные запросы реальных пользователей пропускаются в сеть.

3.5. СХЕМА РАБОТЫ

В рамках данной схемы предоставления сервиса клиент подключается к сети компании «Ростелеком». Вне атаки трафик поступает напрямую клиенту по оптимальному маршруту.

Модуль анализа трафика собирает информацию с маршрутизаторов сети, не пропуская при этом трафик через себя. В случае выявления аномалии анализатор подает сигнал на модуль фильтрации трафика о наличии аномалии и анонсирует на него трафик защищаемого ресурса, очищая его и пропуская при этом легитимные запросы пользователей. После окончания атаки анонс снимается и трафик продолжает поступать напрямую клиенту. Перемаршрутизация трафика клиента на модуль фильтрации занимает не больше минуты. В 80% случаев – до 30 секунд. В некоторых сложных случаях может потребоваться до 3--5 минут.

РИСУНОК 1. СХЕМА ФУНКЦИОНИРОВАНИЯ СЕРВИСА

3.6. КЛЮЧЕВЫЕ ОСОБЕННОСТИ

Сервис мониторинга трафика и защиты от DDoS-атак имеет ряд существенных преимуществ и ключевых особенностей:

- Доставка трафика в отсутствие атаки до защищаемого ресурса без изменения маршрутизации происходит без задержек.
- Фильтрация атак уровня L3/L4 объемом до 5 Тбит/с позволяет отражать даже самые массированные атаки.
- Защита от атак, направленных непосредственно на IP-адрес ресурса (Direct to Origin), без затрат на отдельный выделенный канал.
- Защита серверов доменных имен (DNS), расположенных в инфраструктуре клиента.
- Защита от атак на каналообразующее оборудование (Point-to-point).

3.7. ПРЕИМУЩЕСТВА СЕРВИСНОЙ МОДЕЛИ

Высокий уровень экспертизы

Специалисты компании ГК «Солар» определяют профиль атаки, что позволяет более качественно среагировать на инцидент информационной безопасности. Также эксперты консультируют клиентов по вопросу принятия контрмер.

Круглосуточная доступность

Защита от DDoS-атак и мониторинг трафика осуществляется круглосуточно 7 дней в неделю без перерывов и выходных на всей территории России. Специалистам клиента не требуется отслеживать веб-трафик дополнительно, что высвобождает их время для решения стратегических задач и принятия превентивных мер.

Скорость и оперативность

При необходимости клиент может подключить сервис мониторинга трафика и защиты от DDoS-атак в течение 7 дней. Сервис подключается на определенный клиентом отрезок времени и может быть оперативно масштабирован на все офисы или дочерние предприятия по требованию клиента.

4. ПОДКЛЮЧЕНИЕ И ЭКСПЛУАТАЦИЯ

Сервис представляет собой магистральную защиту от DDoS-атак. Услуга предоставляется непосредственно на каналах оператора связи «Ростелеком». Сервис обеспечивает защиту всей интернет-инфраструктуры клиента и доступность онлайн-ресурсов пользователям круглосуточно.

Сервис мониторинга трафика и защиты от DDoS-атак предоставляется в формате подписки на любой, удобный клиенту период. Эксплуатацию осуществляют высококвалифицированные специалисты компаний «Ростелеком» и ГК «Солар».

Одна из ключевых составляющих сервиса – это личный кабинет с информацией о текущем состоянии трафика клиента в графическом виде.

4.1. ПОРЯДОК ПОДКЛЮЧЕНИЯ СЕРВИСА

Для клиентов сети «Ростелеком» подключение сервиса не требует переконфигурирования клиентского оборудования – все необходимые настройки производятся на оборудовании компании «Ростелеком».

Специалисты «Ростелекома» выполнят проверку сетевой связности роутеров и прохождения трафика, после чего сервис готов к использованию.

Сроки подключения:

- Стандартное подключение к сервису защиты от DDoS-атак осуществляется за неделю и включает три простых шага:

РИСУНОК 2. ЭТАПЫ ПОДКЛЮЧЕНИЯ СЕРВИСА

- В экстренных случаях сервис защиты от DDoS-атак может быть активирован в течение 5 часов после старта работ. Это особенно важно для организаций, которые сталкиваются с внезапными и мощными атаками, поскольку быстрая реакция может минимизировать время простоя и защитить критически важные ресурсы.

4.2. СПИСОК РАБОТ В РАМКАХ ЗАПУСКА СЕРВИСА

Подготовка плана развертывания системы сетевой защиты включает:

- Анализ внутренней ИТ-инфраструктуры компании.
- Выполнение технических работ по подключению клиента к сервису, в частности установку шаблонных параметров анализа трафика.
- Запуск сервиса и предоставление доступа в ЛК ИБ.
- В результате работ по подключению клиент получает готовый к использованию сервис.
- Режим работы технической поддержки: 24×7×365.

4.3. ЭКСПЛУАТАЦИЯ СЕРВИСА

Эксплуатация сервиса осуществляется в режиме 24/7 и включает в себя:

Выполнение работ по администрированию магистральной части системы защиты, в том числе:

1) автоматическое перенаправление трафика на очистку по заранее установленным параметрам;
2) перенаправление трафика на очистку по запросу клиента;
3) корректировку правил фильтрации трафика;
4) выполнение запросов на добавление исключений в работу политик.

Экспертный анализ сетевой активности клиента и развитие оказываемой услуги, состоящие из:

1) доработки существующих сценариев обнаружения атак для снижения количества ложных срабатываний;
2) расширения списка контролируемых сценариев обнаружения атак в рамках внутренних исследований исполнителя;
3) реализации новых сценариев обнаружения и блокирования атак по запросу клиента.

В результате клиент получает передовой для российского рынка и с высоким уровнем защищенности сервис по противодействию DDoS-атакам.

5. О КОМПАНИИ

ГК «Солар» – это архитектор комплексной кибербезопасности. Мы обеспечиваем защиту организаций всех уровней: от малого бизнеса до федеральных органов власти. Ключевые направления деятельности – аутсорсинг ИБ, разработка собственных продуктов, комплексные проекты по кибербезопасности.

Экспертиза, накопленная за годы работы с крупными корпорациями, государственными организациями и объектами критической инфраструктуры, призвана обогащать все наши продукты и поддерживать высокий уровень средств защиты, разработанных с учетом последних видов киберугроз.

В основе подходов и технологий лежит понимание, что настоящая кибербезопасность возможна только через непрерывный мониторинг и удобное управление системами защиты.

№1
на рынке
сервисов ИБ

2000+
экспертов
по кибербезопасности

850+
организаций
под защитой

24/7
обеспечение
кибербезопасности

600+
комплексных и сервисных
проектов в год

200+ млрд
анализируемых
событий ИБ в сутки

Продуктовый портфель ГК «Солар» делится на три основных направления: продукты на базе собственных технологий (DLP, SAST, SWG, IGA), сервисы кибербезопасности под брендами Solar MSS и Solar JSOC, а также услуги в области кибербезопасности, в том числе для защиты автоматизированных систем управления технологическими процессами (АСУ ТП) и Промышленного интернета вещей (IIoT).

6. КОНТАКТНАЯ ИНФОРМАЦИЯ

ТЕЛЕФОНЫ:

+7 (499) 755-07-70 – продажи и общие вопросы

E-MAIL:

solar@rt-solar.ru – продажи и вопросы по сервису

info@rt-solar.ru – общие вопросы

АДРЕСА:

- Москва, Никитский пер., 7, стр. 1
- Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд
- Санкт-Петербург, ул. Савушкина, 126, БЦ «Атлантик Сити»
- Нижний Новгород, Казанское ш., 25, корп. 2
- Самара, Молодогвардейская ул., 204
- Ростов-на-Дону, Доломановский пер., 70Д
- Хабаровск, ул. Серышева, 56
- Томск, Комсомольский просп., 70/1
- Ижевск, ул. Ленина, 21, БЦ «Форум»